IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	CRIMINAL NO. 1:15CR124
	)	
v.	)	Honorable T.S. Ellis, III
	)	
MUNEEB AKHTER,	)	Sentencing Hearing: September 25, 2015
	)	
Defendant.	)	
	)	

POSITION OF THE UNITED STATES WITH RESPECT TO SENTENCING

The United States of America, by and through its attorneys, Dana J. Boente, United States Attorney, and John P. Taddei and Jennifer A. Clarke, Special Assistant United States Attorneys, hereby submits its position with respect to the sentencing of Muneeb Akhter ("defendant"). The government recommends that the defendant receive a sentence of 72 months' imprisonment, which is slightly above the currently calculated advisory Guidelines range (57-71 months), but within the range that results if this Court sustains the government's sole objection to the PSR (63-78 months).

BACKGROUND

On June 26, 2015, the defendant pleaded guilty to six counts of a Criminal Indictment charging him with: Count One—conspiracy to commit wire fraud, in violation of Title 18, United States Code, Sections 1343 and 1349; Count Two—conspiracy to access a protected computer without authorization, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i)-(iii) and 371; Count Seven—access of a protected computer without authorization, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i), (iii); Count Eight—conspiracy to access a government computer without authorization, in violation of Title 18, United States Code, Sections 1030(a)(2)(B) and (c)(2)(B)(i)-(iii) and 371; Count Ten—making

a false statement, in violation of Title 18, United States Code, Section 1001(a)(2); and Count Twelve—obstruction of the due administration of justice, in violation of Title 18, United States Code, Sections 1503 and 3147(1).

Given the breadth of the defendant's relevant conduct and detailed statement of facts supporting his convictions, as well as this Court's in-depth familiarity with the case, the government will not reiterate all of the underlying facts. From in or about March 2014 through in or about March 2015, the defendant, along with coconspirators Sohaib Akhter and Musaddiq Ishaq, orchestrated a scheme to defraud in which they hacked into a cosmetics company run by Ishaq's mother (Victim Company 1) and stole credit card account information belonging to thousands of people. *See* PSR ¶¶ 20-48. The defendant and his coconspirators used the stolen information to make more than $30,000 in fraudulent purchases, which included airline tickets, hotel stays, computers and electronics, sporting equipment, food deliveries, attendance at professional conferences, and more. *See* PSR ¶¶ 30-33, 114. The defendant was the primary architect and facilitator of the scheme. He used key-logger software to secretly record the username and password of a Victim Company 1 employee, which he used to gain access to the company's computer systems. *See* PSR ¶¶ 37-42. He then installed several iterations of complex code onto Victim Company 1's computer systems, which he linked to email accounts that the defendant and his coconspirators used to collect the stolen information. *See* PSR ¶¶ 41-45. In addition to using this information to purchase goods and services, the defendant and a coconspirator that he met on the "dark net" sold some of the information to other dark-net users for $5 per bundle of information. *See* PSR ¶ 48.

In a separate scheme, executed around November 2013, the defendant hacked the computer systems of a data-aggregation company (Victim Company 2) for which he was performing contract

work. *See* PSR ¶¶ 49-63. He did so after the Company's CEO refused to give him free access to proprietary Company information about federal government contracts. *See* PSR ¶ 52. The defendant hoped to use the stolen information to tailor successful bids to win contracts and clients for his and his brother Sohaib's company, Warden Systems. *See* PSR ¶ 53. In addition, the defendant later used his illegal access to insert a code onto the Company's computer systems, which caused the systems to send thousands of mass emails to students at George Mason University asking them to vote for the defendant in an online contest. *See* PSR ¶¶ 60-61. After Victim Company 2's CEO asked the defendant to cease his actions, the defendant threatened the CEO. *See* PSR ¶¶ 62-63.

As part of yet another hacking scheme, the defendant, along with his brother Sohaib and Ishaq, engaged in a series of computer intrusions against the U.S. Department of State to obtain sensitive passport and visa information and other valuable information about State Department computer systems. *See* PSR ¶¶ 64-88. Sohaib Akhter used his contract position at the State Department to illegally access, and in some circumstances download and remove, sensitive passport information belonging to 62 different individuals, including coworkers, acquaintances, the CEO of Victim Company 2, and even a DHS special agent investigating the crimes for which the defendant will be sentenced. *See* PSR ¶¶ 69-75. The defendant requested that his brother access and download much of this information. *See* PSR ¶ 74. The coconspirators specifically targeted the DHS agent's information due to his investigation into their illegal activities. The defendant stated that the agent's information would be "extremely valuable to criminals and that he could either use the information himself or sell it on the 'dark net.'" *See* PSR ¶ 109.

In a separate phase of the State Department conspiracy, Sohaib Akhter attempted to use his access to State Department facilities and computer systems to create an unauthorized account that

would enable him to access those systems undetected. *See* PSR ¶¶ 76-77. He downloaded several programs, including malicious software, in furtherance of the plan. *See* PSR ¶ 77. Sohaib Akhter's specific goal was to achieve remote access to State Department computer systems, and he theorized that if he was successful he could: access information on individuals' passport applications; access and unilaterally approve visa applications without State Department authorization in exchange for payment; and create passports and visas and sell them on the dark net. *See* PSR ¶ 78. After his software-based approach was unsuccessful, Sohaib Akhter spearheaded a plan to secretly install a physical device at a State Department facility that would enable him and the defendant to collect data from and remotely access State Department systems. *See* PSR ¶¶ 79-82. The defendant provided technical assistance for the intrusion by programming the physical device and delivering key components to his brother Sohaib on the day the conspirators executed the attempted installation at the facility. *See* PSR ¶¶ 83-88.

In a separate offense, soon after the defendant was fired as a contractor at DHS for bragging to coworkers about illegally hacking gift cards, he obtained a position with defense contractor Booz Allen Hamilton. *See* PSR ¶ 90. He was able to continue his employment there after he lied on a federally administered national security questionnaire about whether he had ever illegally accessed computer systems and omitted the fact that he had been fired from his DHS contract position. *See* PSR ¶¶ 91-94.

In March 2015, Magistrate Judge Ivan D. Davis released the defendant on conditions of pretrial supervision after he was charged in a criminal complaint with conspiracy to commit credit card fraud. *See* PSR ¶ 95. Following the defendant's release, he obstructed justice by endeavoring to isolate Ishaq from law enforcement officers investigating him and his brother for the crimes detailed here. *See* PSR ¶¶ 96-104. In particular, the defendant paid $1,719 for his coconspirator

Ishaq to leave the United States and even accompanied him to Dulles International Airport to see Ishaq off on his flight to the Republic of Malta. *See* PSR ¶¶ 98-99. While Ishaq was in Malta, the defendant continued to encourage Ishaq to avoid investigators and advised him to travel to Saudi Arabia to stay with the Akhters' father when money became tight. *See* PSR ¶¶ 100-101. When Ishaq returned to the United States and was arrested, the defendant attempted to arrange meetings with Ishaq and continued to advise him to avoid agents. *See* PSR ¶¶ 102-104. The defendant's obstructive activities led this Court to revoke the defendant's bond in May 2015.

The defendant has been detained in the Alexandria Detention Center since his bond was revoked. *See* PSR ¶ 4. His incarceration did not prevent or dissuade him from tampering with additional computer systems. In late-July 2015, the defendant used stolen login credentials to access a restricted area within the Detention Center's law library computer network. *See* PSR ¶ 174. The defendant attempted to hide his activities and, when asked what he was doing, lied that it was legal work. *See id.* The law library was placed on lockdown, and a subsequent investigation revealed that the defendant surreptitiously, and without authorization, created a system that allowed inmates to send private messages to each other. *See id.* At least two other inmates accessed the system. *See id.* The defendant was adjudicated guilty of three major jail violations and sentenced to a period of segregation. *See id.*

PRESENTENCE REPORT AND GOVERNMENT'S OBJECTION

In accordance with Guidelines § 6A1.2 and this Court's policy regarding Guidelines sentencing, the United States hereby represents that it has reviewed the Probation Office's Presentence Investigation Report (PSR) prepared in this matter. The government does not dispute any of the sentencing factors set forth in the PSR or the calculation of the recommended Guidelines range, with one exception.

The government believes that the defendant's PSR should include an additional two-level enhancement under Count Group 1 because the "offense[s] . . . involved sophisticated means." *See* U.S.S.G. § 2B1.1(b)(10)(C). The sophisticated means enhancement applies when a defendant employs "especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense." U.S.S.G. § 2B1.1 cmt. n. 9(B). There is no "require[ment] that the court find the existence of highly complex schemes or exceptional brilliance to justify a sophisticated means enhancement." *United States v. Adepoju*, 756 F.3d 250, 258-59 (4th Cir. 2014).

The Akhter brothers' hack of Victim Company 1 and corresponding theft of thousands of individuals' personal and credit card information "was notably more intricate than that of the garden-variety offense." *United States v. Beckman*, 787 F.3d 466, 496 (8th Cir. 2015) (citation omitted). In particular, they executed and concealed their fraud scheme through sophisticated technical means. The defendant used key-logger software to secretly record the username and password of a Victim Company 1 employee, which he used to gain access to the company's computer systems. *See* PSR ¶¶ 37-42. Then, the defendant installed several iterations of complex code onto Victim Company 1's computer systems, which he linked to email accounts that the defendant, Sohaib Akhter, and other coconspirators used to collect the stolen information. *See* PSR ¶¶ 41-45. The defendant refined the code that he installed so that it "was more difficult to detect than the first code." PSR ¶ 44. This code remained undetected on Victim Company 1 servers for almost a year until it was removed in May 2015. PSR ¶ 47.

This conduct falls squarely within the Sentencing Commission and courts of appeals' conception of what constitutes sophisticated means. *See, e.g.*, U.S.S.G. 2B1.1 cmt. n. 9(B) (citing as an example "hiding assets *or transactions*" (emphasis added)); *United States v. Balde*, 2015 WL

3776392, *4 (4th Cir. June 18, 2015) (unpublished) (evidence that the defendants "obtained hundreds of stolen or fraudulent gift and credit card numbers" and "used many of them by transferring the numbers to stolen cards by use of access device making equipment . . . clearly supported" sophisticated means enhancement); *United States v. Musacchio*, 590 F. App'x 359, 366-67 (5th Cir. 2014) (unpublished) (defendants' use of "administrator accounts to . . . conceal[] their identities" and "forward[ing] the text of [stolen] email using webmail accounts in an attempt to avoid leaving records" supported application of enhancement in Section 1030 prosecution). In its Addendum to the PSR, the Probation Office stated that it "considered the conduct of the defendant in regards to these offenses and made the determination that an enhancement for Use of a Special Skill, pursuant to USSG § 3B1.3, was more appropriate." *See* PSR Add. at 1. However, the defendant did not receive an enhancement for use of a special skill for Count Group 1. *See id.* Even if he had, there is nothing in the Guidelines that would prevent the application of both enhancements where, as here, the defendant used a special skill to perpetrate an offense and engaged in sophisticated means to carry it out or conceal its existence. Thus, this Court should apply a further two-level increase in the defendant's offense level for Count Group 1 based on the defendant's use of sophisticated means to carry out the crimes.

If this Court sustains the government's objection, it will increase the defendant's offense level for Count Group 1 from 24 to 26. *See* PSR ¶ 136. The revision would affect the combined offense level for all counts by reducing the total number of units to one, and thus eliminate the one point increase currently calculated in PSR ¶ 165. *See* U.S.S.G. § 3D1.4 (indicating that if the total number of units is one, there is no increase in the combined offense level). This would result in a total offense level of 26, and, given the defendant's criminal history category of I, a final advisory Guidelines range of 63-78 months' imprisonment.

RESPONSE TO DEFENDANT'S OBJECTIONS

On September 20, 2015, the defendant filed his position with respect to sentencing. The government has the following responses to the objections relevant to the advisory Guidelines calculation:

1. PSR ¶¶ 117, 134—The defendant objected to the application of a two-level enhancement for being an organizer, leader, manager, or supervisor of the fraud and hacking conspiracies included in Count Group 1. The government opposes this objection. When evaluating this enhancement, courts consider factors including "the exercise of decision making authority, the nature of participation in the commission of the offense, the recruitment of accomplices, the claimed right to a larger share of the fruits of the crime, the degree of participation in planning or organizing the offense, the nature and scope of the illegal activity, and the degree of control and authority exercise over others." U.S.S.G. § 3B1.1 cmt. n. 4. The defendant's role in the hacking of Victim Company 1 and use of stolen credit card information relative to the roles of his brother and Ishaq strongly supports this enhancement. It was the defendant—not his codefendants—who placed a key-logger on Victim Company 1 computers, worked with the dark-net coconspirator to insert and modify the codes that forwarded customers' personal and account information, and set up and maintained the email accounts used to collect the information. In particular, the recorded phone conversations—in which the defendant, Sohaib, and Ishaq discuss the defendant's computer intrusions, progress, and initial successful use of stolen credit card information—clearly demonstrate that the defendant was the facilitator of the scheme. Thus, the enhancement is proper.

2. PSR ¶¶ 121, 135—The defendant objected to the application of a two-level enhancement for obstruction of justice included in Count Group 1. The government opposes this

objection. The defendant claimed that the enhancement is improper because the defendant erased computer and cellphone information relevant to the fraud and hacking offenses charged in Counts One and Two after learning of the existence of a *state* warrant to search his residence. He argued that this warrant "was not necessarily" related to his instant *federal* offenses of conviction. The undisputed facts belie this contention. After learning about the state search warrant, which the same federal law enforcement agents involved in the instant case applied for before securing a federal search warrant to search the same residence, the defendant and his brother "erased the contents of their computers and the nsalookup@hotmail.com and credproc@hotmail.com accounts with the purpose of preventing law enforcement from examining them." PSR ¶ 46. Those accounts were used to collect the credit card and personal information stolen from Victim Company 1. Therefore, their contents were unquestionably relevant "to the investigation, prosecution, or sentencing of the instant offense of conviction." U.S.S.G. § 3C1.1.

3. PSR ¶ 125, 168—The defendant argued that he deserves a three-level reduction for acceptance of responsibility. The government opposes this objection. As noted *supra*, the PSR properly applied a two-level enhancement to the defendant's Count Group 1 offense level for obstruction of justice. "Conduct resulting in an enhancement under § 3C1.1 . . . ordinarily indicates that the defendant has not accepted responsibility for his criminal conduct." U.S.S.G. § 3E1.1 cmt. n. 4; *see United States v. Knight*, 606 F.3d 171, 175 (4th Cir. 2010) (noting a defendant may receive both an enhancement for obstruction *and* a reduction for acceptance of responsibility only in "extraordinary cases"). In addition, as reflected in Count Twelve, the defendant continued to obstruct the investigation into the criminal conduct underlying Count Group 1 after he was charged for the same fraudulent conduct in a criminal complaint and released on bond pending trial. The defendant argued that "§ 3E1.1 addresses instances of obstructive behavior *following* a plea

agreement." The Fourth Circuit has rejected this argument. *See Knight*, 606 F.3d at 176 (noting "[t]o the extent that [defendant] is arguing for the application of a bright-line rule that an acceptance-of-responsibility reduction should be applied so long as the defendant does not obstruct justice *after* agreeing to plead guilty . . . her position is inconsistent with our case law"). We should note that after pleading guilty, the defendant conducted multiple proffer sessions with the government in which he detailed his criminal conduct and confirmed the roles of others within the various conspiracies. However, we should also note that the defendant's plea agreement required him to participate in these sessions. On balance, given the defendant's history of obstructive conduct related to the investigation into the charges contained in Count Group 1, the government does not believe that this represents one of the "extraordinary cases" where both an obstruction enhancement and a reduction for acceptance apply.

4. PSR ¶ 138—The defendant objected to the loss-amount calculation for Count Seven, arguing that it should be $5,000-6,500 rather than $13,950. The government opposes this objection. As the defendant swore in his Statement of Facts, "Victim Company 2 charged customers more than $13,000 for the access that [the defendant] secured" through his hack of the Company's systems. PSR ¶ 55. Because the intended loss was more than $10,000 but less than $30,000, the Probation Office properly applied a four-level enhancement pursuant to U.S.S.G. § 2B1.1(b)(1)(C).

5. PSR ¶¶ 118, 140, 148—The defendant objected to the application of a two-level enhancement for use of a special skill for Counts Seven and Eight. The government opposes these objections. The Guidelines define a "special skill" as "a skill not possessed by members of the general public and usually requiring substantial education, training or licensing." U.S.S.G. § 3B1.3 cmt. n. 4. There is no question that the defendant's advanced hacking and computer skills

are not possessed by the general public. The defendant is a self-proclaimed "cybersecurity ninja" with a bachelor's degree in electrical engineering and a master's degree in computer engineering from George Mason University. *See* PSR ¶¶ 188, 190. He possess numerous certificates for a wide variety of complex computing abilities and his skills have enabled him to secure coveted positions at established organizations and companies including Booz Allen Hamilton, General Dynamics, Airbus, and the Department of Homeland Security. *See* PSR ¶¶ 189-190. As detailed *supra,* the defendant exercised these skills in hacking Victim Company 2 and participating in the conspiracy to hack the State Department. In fact, he admitted to the Probation Office, "Without authority, I improperly used my advanced computer training and skills to access and obtain information I should not have had." PSR ¶ 124. Thus, the enhancement is proper.

6. PSR ¶ 163—The defendant argued that all counts of conviction should be grouped together. The government opposes this objection. The Probation Office fully and accurately explained why the grouping of offenses contained in the PSR is appropriate and therefore we need not further address the issue here. *See* PSR Add. at 5.

SENTENCING RECOMMENDATION

There is little question that the defendant possesses considerable talent with computers. What he has chosen to do with that talent, and his continued inability to follow the law and other important rules and regulations, demonstrate that a significant term of imprisonment is necessary in this case.

Between Fall 2013 and Spring 2015, the defendant either personally hacked or substantially assisted in hacking two separate companies and the U.S. Department of State. In the first scheme, the defendant facilitated the theft of credit card and personal information belonging to thousands of individuals. Along with his brother Sohaib and other coconspirators, the defendant used the

stolen information to purchase personal items including food orders, sporting equipment, computers and electronics, flights across the United States, and attendance at technical conferences. He even went so far as to sell bundles of people's personal information to anonymous users on the dark net for as little as $5 per bundle without regard to the danger that it could present to those individuals. Recorded conversations illustrated that the defendant treated theft and the use of others' personal information as little more than a game or activity. In many circumstances, the defendant used stolen information simply to test what he could get away with. This conduct demonstrates a troubling indifference to the sanctity of an individual's most personal information—including one's name, address, and credit.

The defendant's hack of Victim Company 2 also demonstrates his cavalier approach to electronic boundaries and his lack of concern for the impact of his conduct. When the CEO of Victim Company 2 told him that he could not access the company's valuable database of federal data for free, the defendant stole the CEO's login credentials and created his own workaround. The defendant's goal was to use the Company's proprietary information for the benefit of his and his brother's own company. There was no consideration for the fact that he was stealing from his own employer. Nor did the defendant appreciate the havoc that he caused when he inserted a code onto Company servers that caused them to send thousands of emails to George Mason students. This act is particularly glaring given its comparatively inconsequential purpose—to marshal votes for an online contest that the defendant had entered. Perhaps most troubling is that when the CEO confronted the defendant about the unauthorized access, the defendant threatened him, stating "[a]ggression may leave us and our companies both in a bad position" because "[t]he authorities who may put me on trial will also revoke access to your data." PSR ¶ 63.

A conversation between the defendant and his brother Sohaib in June 2014, soon after the defendant landed a cybersecurity job at DHS, reflects an even more concerning philosophy toward government computer systems.

> Sohaib Akhter: You gotta case the joint. You gotta figure out exactly what's happening here and there and have an elaborate scheme built out that you'll never leave a trace.
>
> MUNEEB AKHTER: Yeah, you first climb the ladder. Know your shit. Need to know who's watching. Luckily I'm one of the people that are watching, so I know what kind of evades.
>
> Sohaib Akhter: Yeah, but I'm pretty sure they have insider protection methods and you gotta figure that shit out.
>
> MUNEEB AKHTER: Yeah.
>
> Sohaib Akhter: Best not to be the first person to do shit. See around, do it for probably a year or so, make sure that other people . . . .
>
> MUNEEB AKHTER: We get access to a lot of different viruses, malware strains, just because you're watching the packets and you see that this thing is malicious and you can download their binaries, their weird malware. Wonder if you could really retool it such that it becomes a weapon on your part.

PSR ¶ 66.

The hack of the State Department several months later demonstrated that the Akhter brothers were willing to go beyond mere theorizing and actually exploit weaknesses in government computer systems. Although Sohaib Akhter was the primary facilitator of the State Department hack, he often acted at the request of his brother to look up passport information pertaining to specific individuals. The Akhters boldly accessed and removed a federal agent's information—which included his picture, address, and other sensitive identifying information—in retaliation for the agent's ongoing investigation into their crimes. They also tried to access another case agent's information, but failed because they did not know his real first name. The defendant showed particular vindictiveness when he threatened to release the agent's information to the world, telling

Ishaq that it would be "extremely valuable to criminals and that he could either use the information himself or sell it on the 'dark net.'" *See* PSR ¶ 109.

Sohaib Akhter also mentioned the possibility of selling State Department information, telling Ishaq that if his plan to achieve remote access was successful, he could access information on individuals' passport applications; access and unilaterally approve visa applications without State Department authorization in exchange for payment; and create passports and visas and sell them on the dark net. *See* PSR ¶ 78. The defendant went along with his brother's plan, programming the physical device that Sohaib attempted to install behind a wall at a State Department facility. The plan only failed because Sohaib did not have the proper equipment and broke the device during installation.

Other actions reflect the defendant's troubling pattern of disregard for the law and other rules. First, after being fired from his position at DHS, the defendant lied in order to secure employment at defense contractor Booz Allen Hamilton. As exemplified by his conduct, the defendant posed a great risk to the integrity of Booz Allen's computer systems, and his false statements on the government's main national security background check left Booz Allen dangerously in the dark regarding his firing and past illegal activities. Furthermore, the defendant's repeated efforts while he was on pretrial release to obstruct justice by keeping Ishaq from government investigators again illustrate the defendant's complete lack of respect for the law and judicial authority.

Finally, it is important to note that not even incarceration could deter the defendant from engaging in unauthorized and dangerous conduct with computers. In July 2015, several months into his time at the Alexandria Detention Center after this Court revoked his bond in May, the defendant stole a jail administrator's password and used it to surreptitiously create an unauthorized

and secret inmate messaging system on jail computers. The danger of a system that inmates could use to communicate with one another in secret without the knowledge of jail officials is obvious.

Title 18, United States Code, Section 3553(a) states that this Court should consider the nature and circumstances of the offense and characteristics of the defendant. This Court must also consider other factors, including the need for the sentence "to reflect the seriousness of the offense, to promote respect for law, and to provide just punishment for the offense; [and] to afford adequate deterrence to criminal conduct." 18 U.S.C. § 3553(a)(2)(A) & (B). In addition, the sentence should protect the public from further crimes of the defendant and provide the defendant with needed correctional treatment. 18 U.S.C. § 3553(a)(2)(C) & (D). Finally, the sentence should address "the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct." 18 U.S.C. § 3553(a)(6).

Even though the Sentencing Guidelines are advisory, *United States v. Booker*, 543 U.S. 220 (2005), provides that sentencing courts "must consult those Guidelines and take them into account when sentencing." *Id.* at 264. "[A] district court shall first calculate (after making the appropriate findings of fact) the range prescribed by the guidelines. Then, the court shall consider that range as well as other relevant factors set forth in the guidelines and those factors set forth in [18 U.S.C.] § 3553(a) before imposing the sentence." *United States v. Hughes*, 401 F.3d 540, 546 (4th Cir. 2005).

The government submits that a sentence of 72 months' imprisonment will reasonably and appropriately account for all the factors set forth in 18 U.S.C. § 3553(a). As argued *supra*, the government contends that the properly calculated advisory Guidelines range is 63-78 months' imprisonment. But even if the district court denies the government's objection, the government contends that a sentence slightly above the PSR's advisory Guideline's range of 57-71 months'

imprisonment is warranted. As an initial matter, based on the Guidelines' grouping rules, the defendant's convictions in Counts Seven, Eight, and Ten currently have no impact on his advisory Guidelines range. *See* PSR ¶ 163. The inclusion of Count Twelve only results in a one-point increase in the defendant's offense level. *See* PSR ¶ 165. Thus, the majority of the defendant's illegal conduct—including his hack of Victim Company 2, his participation in the conspiracy to hack into the State Department, his false statements on the national security questionnaire, and even his obstructive activity related to Ishaq—has either little or no impact on his Guidelines range. As the Guidelines set forth, this circumstance "may provide a reason for sentencing at the higher end of the sentencing range for the applicable offense level." U.S.S.G. § 3D1.4(c).

Furthermore, both the wide range of the defendant's criminal conduct and the depth of its seriousness signifies that a significant term of imprisonment is necessary in this case. A 72-month sentence would promote respect for the law for a defendant who repeatedly engaged in obstruction of justice and even manipulated computer systems while in jail. It would also communicate the seriousness of the offenses and serve a strong deterrent effect, not just for the defendant, but also for other individuals who might consider engaging in similar conduct. This is especially important at a time when computer hacking, in particular hacking of government and corporate computer systems, presents a growing problem in the United States. Finally, the defendant's repeated misuse of his computer skills demonstrates that he remains a substantial threat to the personal security of numerous individuals, as well as a threat to national security.

CONCLUSION

For all of the above reasons, the United States respectfully submits that a sentence of 72 months' imprisonment would be sufficient, but not greater than necessary, to accomplish the goals of 18 U.S.C. § 3553(a).

Respectfully submitted,

Dana J. Boente
United States Attorney

_____/s/_____
John P. Taddei
Special Assistant United States Attorney (LT)

_____/s/_____
Jennifer A. Clarke
Special Assistant United States Attorney (LT)

CERTIFICATE OF SERVICE

I hereby certify that on September 21, 2015, I electronically mailed a copy of the foregoing to Joseph McCarthy and Mark Petrovich, the attorneys of record for the defendant.

_____/s/_____
John P. Taddei
Special Assistant United States Attorney